Servizio Sanitario Nazionale
Regione Piemonte

Azienda Ospedaliera
Ordine Mauriziano di Torino

Deliberazione del Direttore Generale

Oggetto: **Applicazione Circolare 18 aprile 2017 , n. 2/2017 «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».**

IL DIRETTORE GENERALE

Dott. Silvio FALCO, nominato con D.G.R. n. 43-1371 del 27.04.2015;

su conforme proposta del Direttore della SC I.C.T. e Sistemi Informativi, Dott.ssa Silvia Torrengo, che ne attesta la legittimità e la regolarità sostanziale e formale di quanto di seguito indicato

Premesso che l'art. 14 -bis del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera a) , tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

Premesso che la direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

Premesso che la Circolare 18 aprile 2017 , n. 2/2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto

2015)», sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017).

Premesso che l'obiettivo della suddetta circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi. Le misure minime di cui al comma precedente sono contenute nell'allegato, che costituisce parte integrante della circolare unitamente alle modalità con cui ciascuna misura è implementata presso l'amministrazione

Dato atto che le Amministrazioni destinatarie della suddetta circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D e che entro il 31 dicembre 2017 tali amministrazioni dovranno attuare gli adempimenti richiesti dalla Circolare. Nella sotto riportata tabella sono sintetizzate le misure minime di sicurezza ICT per le pubbliche amministrazioni secondo i tre livelli previsti:

- «Minimo», specifica il livello sotto il quale nessuna amministrazione può scendere e tali controlli sono obbligatori
- «Standard», specifica il livello che deve essere assunto come base di riferimento nella maggior parte dei casi
- «Alto», specifica il livello a cui tendere.

	Circolare Agid			**Mauriziano al 31.12.2017**		
Tipologia Misure	**Livello Minimo**	**Livello Standard**	**Livello Ato**	**Livello Minimo**	**Livello Standard**	**Livello Ato**
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	3	5	5	3	5	4
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	2	3	3	2	3	2
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER	3	3	5	3	3	1
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	7	11	1	7	7	0
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	12	11	3	12	10	1
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE	11	8	4	11	8	4
ABSC 10 (CSC 10): COPIE DI SICUREZZA	3	1	2	3	1	2
ABSC 13 (CSC 13): PROTEZIONE DEI DATI	2	1	8	2	1	4
Totale	**43**	**43**	**31**	**43**	**38**	**18**
				100%	88%	58%

Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono fornire un adeguato livello di protezione e devono essere affiancate da efficaci strumenti di rilevazione, in grado di abbreviare i tempi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte. A tal fine sono stati individuati anche gli interventi/forniture idonee per l'adeguamento delle misure a disposizione dell'Azienda Mauriziano per incrementare la percentuale di raggiungimento delle Misure di "livello Standard (oggi 88%) e delle Misure di "Livello Alto" (oggi 58%), che saranno oggetto di Deliberazioni nel corso del 2018.

Considerato che nella sezione "*ABSC 4 (CSC 4): Valutazione e correzione continua della vulnerabilità"*, è prevista la definizione di un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.)

Dato atto che la norma UNI CEI ISO 27001 è una norma internazionale che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa di un'Azienda. La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione e include anche i requisiti per la valutazione e per il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. A tal fine è stato predisposto un documento "Risk Assessment Report" , allegato come parte integrante e sostanziale al presente provvedimento, che permette:

- l'individuazione/identificazione dei rischi che incombono sulla sicurezza delle informazioni
- la valutazione dei rischi
- l'identificazione e valutazione delle opzioni per il trattamento dei rischi
- la scelta degli obiettivi di controllo ed i controlli per il trattamento dei rischi
- l'analisi dei rischi

Acquisito il parere favorevole del Direttore Sanitario e del Direttore Amministrativo ai sensi dell'art. 3 del D.Lvo 502/92 e successive modifiche ed integrazioni;

Dato atto della vigente normativa richiamata e/o riferita al presente provvedimento;

DELIBERA

1. Di approvare, ai sensi dell'art. 4 della Circolare 18 aprile 2017 , n. 2/2017 «Misure minime di sicurezza ICT per le pubbliche amministrazioni», il modulo di implementazione delle misure, firmato digitalmente dal Direttore della S.C. I.C.T. & Sistemi Informativi e dal rappresentante legale dell'Azienda Ordine Mauriziano di Torino, nel testo allegato al presente provvedimento quale parte integrante e sostanziale;

2. Di approvare, il Piano di gestione dei Rischi “Risk Assessment Report” dell'A.O. Ordine Mauriziano di Torino, allo scopo di individuare le vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici, nel testo allegato al presente provvedimento quale parte integrante e sostanziale

3. Di dare atto che per l'attuazione di tutte le misure minime previste sarà necessario attivare nuovi interventi/forniture nel corso del 2018 e che pertanto la rilevazione attuale sarà oggetto di aggiornamento, finalizzato alla attuazione ed al miglioramento delle suddette misure

4. Di dare atto che dal presente provvedimento non derivano oneri per l’Azienda;

5. Di dichiarare il presente provvedimento immediatamente esecutivo ai sensi dell’art. 28 della legge regionale 24/01/1995, n. 10.